SECURE PRINTER CARTRIDGE

BACKGROUND OF THE INVENTION

[001] The present invention relates to an inkjet printer cartridge including at least one print head for printing data on a support.

[002] In the field of printing, printer units such as printers that include at least one monochrome or color printer cartridge are used in a manner that is known to the person skilled in the art for inkjet printing of data onto a support such as a sheet of paper.

[003] On the inkjet printer cartridge there is usually a thin printed circuit including electrical contact areas connected by conductive tracks to a print head provided with nozzles for ejecting ink.

[004] The printer unit includes a carriage forming a cartridge support and on which the printer cartridge is installed, the carriage moving in translation to print data onto a sheet of paper. This is known in the art.

[005] The printer unit also includes a printing management electronic circuit card connected to the carriage by a ribbon cable.

[006] When the printer cartridge is installed on the carriage, the electrical contact areas thereof are in contact with contact areas of the ribbon cable connecting the carriage to the card.

[007] Accordingly, printing commands from the printing management electronic circuit card are transmitted via the ribbon cable and reach the contact areas of the thin printed circuit on the cartridge, where they are routed directly to the print head to control the printing of data.

[008] The thin printed circuit on the cartridge is a passive circuit and guarantees continuity of the electrical signals transmitted to the cartridge.

[009] These printer cartridges which are available off the shelf are entirely standardized consumable products whose service life is generally of the order of a few months.

[0010] The data transmitted to the printer cartridge is sometimes deemed to be sensitive, for example because it is confidential or represents sums of money.

[0011] The latter situation is encountered, for example, in the field of franking

machines, where franking data representative of a monetary value is transmitted from a unit that generates the data to a printer unit for printing the franking data on an envelope.

[0012] Accordingly, in this field, as in all other fields in which sensitive data is printed on a support, the problem arises of securing data during transfer of data between the source of sensitive data and the printer cartridge.

[0013] To this end, the data can be encrypted in the source, for example, and decrypted in the printer unit before transmitting it to the printer cartridge.

[0014] However, the decrypted data can nevertheless still be intercepted by a fraudster.

[0015] It would be equally possible to provide a specific printer cartridge that includes a data decrypting circuit and that is rendered inaccessible from the outside, for example by embedding it in resin.

[0016] However, this necessitates modification of the printer cartridge and even the printing system itself.

[0017] The problem of securing data is therefore even more difficult to solve when the technology of the printer cartridges and the corresponding printer units must not be called into question and when it is preferable to be able to continue to use printer cartridges and printer units available off the shelf.

[0018] It would therefore be beneficial to be able to secure sensitive data to be printed without modifying the printing technology.

SUMMARY OF THE INVENTION

[0019] To this end, the invention proposes an inkjet printer cartridge including at least one print head for printing data on a support, characterized in that a thin printed circuit is permanently fixed to the printer cartridge and a miniature data processing unit fixed to said printed circuit analyzes a stream of printing commands for controlling the print head to authenticate the data to be printed on the support.

[0020] By fixing the printed circuit to a standard printer cartridge, the processing unit attached to said circuit is able to analyze printing commands and more particularly to control the validity of data that might have been tampered with before reaching the

cartridge.

[0021] Because the printed circuit and the processing unit are thin, this is possible without having to modify the shape of the cartridge and the cartridge support.

[0022] The circuit and the processing unit therefore add very little to the overall bulk of the printer cartridge equipped in this way.

[0023] Moreover, it would be virtually impossible for a fraudster to insert any kind of equipment between the circuit and the printer cartridge, given that they are fastened together and that the circuit would be damaged if any attempt were made to remove it.

[0024] The invention therefore improves the security of data compared to the prior art.

[0025] Moreover, authenticating data to be printed authenticates the sender of the data.

[0026] According to one feature, the printed circuit is flexible, i.e. it bends easily.

[0027] This can be particularly advantageous if the circuit has to be fixed to a non-plane surface of the cartridge.

[0028] According to another feature, the processing unit includes means for verifying the presence in the stream of printing commands of data for authenticating data to be printed.

[0029] Authentication data is inserted into the stream of data to be printed and, for example, is extracted by the processing unit to verify its authenticity.

[0030] According to one feature, the processing unit includes means for verifying the integrity of data to be printed to ensure that it has not been intercepted and tampered with by a third party.

[0031] This constitutes an additional degree of security.

[0032] According to one feature, the processing unit includes means for deciding whether or not to authorize the printing of data according to the result obtained by the verification means.

[0033] Accordingly, in the event of a positive verification result, it is decided to authorize printing of the data to be printed but the authentication data itself will not be printed.

[0034] On the other hand, if the printing data has been tampered with (negative

verification result), the processing unit will decide not to print the data, or to print the data incompletely or with a mark indicating that the printing is not authorized.

[0035] According to one feature, the energy necessary for the processing unit to function is obtained from the stream of printing commands.

[0036] Accordingly, with the invention, it is not necessary to provide a source of energy on the printed circuit, which simplifies its structure and reduces its manufacturing cost.

[0037] This aspect of the invention is therefore particularly advantageous in that the manufacturing cost of the printed circuit is relatively low compared to that of a standard printer cartridge.

[0038] Furthermore, the self-powering of the processing unit guarantees a certain independence from the printing system.

[0039] According to one feature, the data processing unit is implemented in programmed logic, which reduces power consumption and therefore diverts as little energy as possible from the stream of printing commands. Diverting too much energy from the stream of printing commands would visually degrade the printed data.

[0040] The data processing unit could use a microprocessor provided that there is no risk of the energy diverted from the stream of printing commands degrading the printing of data.

[0041] According to one feature, the printed circuit is glued to the exterior surface of the printer cartridge.

[0042] Nevertheless, the circuit can equally be fixed by other means, such as by welding or by any other mechanical fastening means.

[0043] According to one feature, in known manner the cartridge has on its exterior surface electrical contacts connected to the print member in order to transmit to it printing commands for printing data on the support.

[0044] According to another feature, the printed circuit has a first portion carrying electrical contacts adapted to receive the stream of printing commands and connected to the data processing unit and which is on a first region of the exterior surface of the cartridge.

[0045] According to one feature, the printed circuit has a second portion on which

the data processing unit is mounted and which is on a second region of the exterior surface of the printer cartridge.

[0046] The printed circuit needs to be flexible if the two regions of the exterior surface of the cartridge are not in the same plane or if one of the regions is not plane.

[0047] According to one feature, the second portion of the printed circuit is on a second region of the exterior surface of the printer cartridge which, when said printer cartridge is integrated into a printer unit, forms with the components of said unit sufficient space to accommodate the data processing unit.

[0048] The circuit and the processing unit are therefore optimally adapted to the shape of the cartridge and the cartridge support in the printer unit.

[0049] According to one feature, the printed circuit is double-sided, which reduces its overall bulk.

[0050] According to one feature, one of the faces of the circuit in contact with the cartridge includes electrical contact areas connected to the electrical contacts connected to the print head and to the data processing unit on the opposite face of the circuit.

[0051] Thus the circuit is perfectly adapted to the existing technology of printer cartridges as it has means for interfacing it to the cartridge.

[0052] According to another feature, the opposite face carrying the data processing unit includes electrical contacts adapted to receive the stream of printing commands.

[0053] According to one feature, the data processing unit is thin, so that it does not modify the overall bulk of the cartridge adapted in this way.

[0054] According to one feature, the total thickness of the processing unit and the printed circuit is less than or equal to 1.5 mm.

[0055] The invention also provides a data printing unit that includes an inkjet printer cartridge conforming to the foregoing brief description.

[0056] Thus the invention secures in a very reliable manner the printing of sensitive data without calling into question the printing technology.

[0057] The invention also provides a franking machine including a unit for generating franking data to be printed and a printer unit receiving franking data from the

franking unit, characterized in that the printer unit includes an inkjet printer cartridge conforming to the foregoing brief description.

[0058] Thus the invention secures franking machines in a very reliable manner without calling into question the printing technology.

DESCRIPTION OF THE DRAWINGS

[0059] Other features and advantages of the invention will become apparent in the course of the following description, which is given by way of nonlimiting example only, and with reference to the appended drawings, in which:

[0060] Figure 1 is a diagrammatic representation of the architecture of a franking machine including a printer cartridge according to the invention;

[0061] Figure 2 is a diagrammatic view of an identification module 58 of a printer cartridge according to the invention;

[0062] Figures 3a and 3b are diagrammatic views of two opposite faces of an intelligent module 54 of a printer cartridge according to the invention;

[0063] Figures 4a to 4h show successive operations of fitting out a printer cartridge according to the invention;

[0064] Figure 5 is a diagrammatic view of the data processing unit of the intelligent module 54 of Figure 3;

[0065] Figure 6 is a more detailed view of the unit 68 of the data processing unit of Figure 5;

[0066] Figure 7 is a detailed diagrammatic view of the self-powering unit 92 from Figures 5 and 6; and

[0067] Figure 8 shows timing diagrams of various signals for generating a self-powering signal Vout.

DETAILED DESCRIPTION

[0068] The embodiment shown schematically in Figure 1 represents the general architecture of a franking machine 10 integrating a printer cartridge according to the invention.

[0069] This machine generally includes two entities: a unit 12 for generating

franking data and a unit 14 for printing data that receives franking data from the unit 12 in order to print it, for example in the form of a franking mark 16 on an envelope 17.

[0070] To be more specific, the unit 12 has the following functions:

[0071] composing the franking mark;

[0072] sending data to be printed to the printer unit 14 (scheduling printing of the franking mark);

[0073] managing accounting data, in the sense of managing the totalizing counter of franking amounts and imprint counters;

[0074] checking the consistency of the accounting data, which ensures the reliability of the data record for each franking cycle; and

[0075] guaranteeing the integrity, confidentiality and availability of the accounting data.

[0076] As shown in Figure 1, the unit 12, also known as a meter, includes a central data processing unit 18 that communicates with a module 20 including a cryptographic circuit 22 containing the algorithm or algorithms necessary for encrypting data, a fraud detector circuit 24 which, for example, detects attempted opening of the cover of the franking machine, for example, by means of mechanical or optical contacts, for example, and a CSP circuit 26 that is informed of attempted fraud by the circuit 24 and then deletes critical data such as the encryption keys or algorithms, for example.

[0077] The unit 12 also includes a modem 28 enabling the postal services to read the meters of the franking machine by telephone, for example for billing purposes.

[0078] The central unit 18, which includes in particular a processor or microprocessor, also communicates with scales 30 for weighing postal packets to be franked.

[0079] Figure 1 also shows other external devices, for example a device 32, such as an electronic circuit card (PC option), for example, for emulating the man-machine interface (MMI) 36 integrated into the franking machine 10, and which conventionally includes a keyboard and a screen (not shown).

[0080] The unit 12 for generating franking data communicates with the printer unit 14 via a communication mode, for example, of cable type which is based on a USB connection 38.

[0081] Data and signals are exchanged, in known manner, between the other components of the franking machine and with external devices via cable connections.

[0082] The central unit 18 communicates in particular with the module 20, the external devices 30, 32, and the man-machine interface 36 via cable connections.

[0083] The printer unit 14, which is a printer, for example, includes a printing control module 40 which receives from the unit 12 a stream of franking data to be printed and an encrypted signature 42 and converts the data received into a stream of printing commands 44 that is then sent to one or more printer cartridges 46 for printing franking data in the form of the franking mark 16.

[0084] To be more specific, the printer cartridge 46 includes an ink reservoir 48 and a print head 50 for printing data (Figures 1 and 4a).

[0085] The commands for printing the stream 44 control the print head 50 for printing the franking mark 16 on the support 17.

[0086] The printer cartridge 46 is rendered intelligent by the presence of a module 54 affixed to it and described in more detail later.

[0087] The franking machine 10 further includes additional wireless communication means between the printer cartridge 46 and the unit 12, enabling the latter to identify said printer cartridge.

[0088] To be more specific, the unit 12 includes a sender module 56 and the printer unit 14 includes a receiver module 58 affixed to the printer cartridge 46.

[0089] In this embodiment, wireless communication between the unit 12 and the printer cartridge 46 is performed via radio waves.

[0090] The module 58 sends data identifying the printer cartridge to the unit 12.

[0091] In this embodiment, the module 58 is a tag identifying the printer cartridge which communicates its identification data by radio when acted on by an electromagnetic field whose source is in the module 56.

[0092] When the module 56 wishes to identify a print member in order to check that it is an authorized printer cartridge, it then generates a constant magnetic field directed to the module 58 of the printer cartridge 46 and, by means of a receiver circuit, measures variations in the magnetic field generated by the module 58.

[0093] The module 58 amplitude-modulates the electro-magnetic signal, so to

speak.

[0094] Thus measuring the variations of the electromagnetic field provides data identifying the printer cartridge and therefore enables the nearby printer cartridge to be recognized or not.

[0095] This recognition procedure is carried out before the unit 12 for generating data sends franking data to the printer unit 14 for printing.

[0096] The frequency of the electromagnetic waves emitted by the module 56 is 13.56 MHz, for example.

[0097] This remote communication and identification technology is known as radio frequency identification (RFID).

[0098] Note that the module 56 may require to write data in the identification module 58 and to this end the amplitude modulation of the electromagnetic signal is then generated directly by the module 56 itself.

[0099] Note also that the identification tag 58 is known as an RFID tag.

[00100] To be more specific, the module 56 is, for example, an electronic component commercialized by Texas Instruments under the commercial reference HF reader system series 6000 S6700 Multi-protocol Transceiver IC.

[00101] This kind of component, also known as a transponder, manages the exchange of data and signals between the identification tag 58 and the transponder itself.

[00102] The identification tag is, for example, commercialized by Texas Instruments under the reference Tag-It HF-1 Transponder Inlay Rectangle - Miniature.

[00103] This component has a memory space of 2 kbits accessible in read mode and in write mode and contains for each component a unique identification number (main identification data) that is accessible only in read mode.

[00104] Once the identifier has been stored in the tag, it is therefore no longer possible to modify it.

[00105] When the tag is affixed permanently to a printer cartridge, the identifier of the tag constitutes a unique identifier of the printer cartridge itself.

[00106] The identification tag also contains secondary identification data that relates, for example, to the use of the cartridge in a given application, i.e. in a franking

machine in the embodiment described here.

[00107] In the context of using the printer cartridge in a data printer unit of a franking machine, secondary identification data can be specific to the franking applications, for example.

[00108] Figure 2 shows highly schematically an identification tag used in the Figure 1 franking machine 10. Note, however, that a tag of this kind intended to be affixed to an inkjet printer cartridge provided with a print head according to the invention can be used outside the field of franking machines, more generally in printer units that receive confidential and/or sensitive data from external devices.

[00109] The presence of the identification tag on a printer cartridge of a printer unit of the above kind secures the printing of confidential and/or sensitive data in that authorization to print such data is accorded only if the printer cartridge has been identified unambiguously, by means of its identification tag, during a recognition procedure executed between the source of the confidential and/or sensitive data and said print member.

[00110] Referring again to Figure 2, the identification tag 58 includes a substrate 60 that is thin and flexible, i.e. one that bends easily, on which are provided radio communication means constituting the communication function of the identification tag. The communication means consist of an integrated circuit 62 that implements the send and receive function and an antenna 64 that picks up the magnetic field.

[00111] In the above example of an identification tag the antenna 64 is at the periphery of the substrate 60, for example.

[00112] Figures 3a and 3b show diagrammatically the module 54 constituting the onboard intelligence of a printer cartridge according to the invention.

[00113] The module 54 takes the form of a thin double-sided printed circuit that is flexible, i.e. one that bends easily, to which is attached a thin miniature data processing unit 68.

[00114] The total thickness of the thin circuit 66 and the processing unit 68 must be sufficiently small that, when the intelligent module 54 is fixed to a standard inkjet printer cartridge 46, as described hereinafter with reference to Figures 4a to 4h, the bulk of the cartridge equipped in this way does not compromise the installation of the cartridge in

the standard printer unit for which it is intended.

[00115] It is important that, when integrated into the printer unit, the printer cartridge forms with the components of the printer unit sufficient space to accommodate the circuit 66 equipped with the data processing unit 68.

[00116] The total thickness of the circuit 66 and the unit 68 is less than 1.5 mm, for example, enabling it to be integrated with a very large number of inkjet printer cartridges without modifying the geometry of the cartridge and its support.

[00117] The thickness of the data processing unit 68 is around 1 mm, for example (e.g. 0.9 mm), and that of the circuit 66 is less than 0.2 mm, for example.

[00118] However, for some applications where the overall size constraints relating to the installation of the cartridge on its support are less severe, a total thickness of the circuit 66 and the unit 68 from 1.5 to 2 mm can be envisaged, for example.

[00119] As shown in Figure 3a, the circuit 66 includes on a front face a plurality of electrical contact areas 70a to 70k adapted to communicate with the processing unit 68 via respective conductive tracks 72a to 72k.

[00120] The contact areas 70a to 70k therefore receive the stream of printing commands 44 from the Figure 1 printing control module 40 and send it to the processing unit 68.

[00121] As shown in Figure 3a, the circuit 66 includes a plurality of conductive tracks that run from the processing unit 68 (in the bottom left-hand corner) to the opposite, rear face of the double-sided circuit, which is shown in Figure 3b.

[00122] The circuit 66 has on the rear face a plurality of electrical contact areas 73a to 73k which are connected to the processing unit 68 via respective conductive tracks 75a to 75k that are partially represented in the left-hand portion of Figure 3a and adapted to come into contact with the corresponding electrical contact areas 79 on the standard printer cartridge 46 shown in Figure 4a.

[00123] Accordingly, after having analyzed the stream of printing commands 44 received via the electrical contact areas 70a to 70k, the processing unit 68 sends the commands successively via the conductive tracks 75a to 75k, the electrical contact areas 73a to 73k, and the corresponding electrical contact areas on the Figure 4a printer cartridge, until they finally reach the print head of the cartridge, in order to control

the printing operation.

[00124] Note that the Figure 3a flexible circuit 66 has two portions that are delimited by two facing notches 74 and 76 on two parallel longitudinal edges of the support and define a bending line between those portions. As described later with reference to Figures 4e to 4h, the bending line allows the module 54 to be installed on two different regions of the exterior surface of the printer cartridge.

[00125] The printed circuit 66 has a first portion 67 carrying the electrical contact areas 70a to 70k and a second portion 69 carrying the processing unit 68.

[00126] Note that the processing unit 68 is implemented in programmed logic, which reduces its energy consumption.

[00127] The flexible printed circuit is made from a PTF polymer material approximately 0.125 mm thick, for example.

[00128] Note that the PTF technology employed is relatively economical and uses a polyester film for the dielectric and a silver-containing conductive ink to produce the conductive track previously cited.

[00129] This technology can produce multilayer circuits.

[00130] The data processing unit 68 is mounted on the printed circuit 66 by means of techniques known to the person skilled in the art for integrating an electronic component onto a circuit.

[00131] For example, the unpackaged component can be integrated into a TSSOP approximately 0.9 mm thick.

[00132] The component protected by its packaging is then transferred to the circuit by a technique known to the person skilled in the art and the connecting pins of the packaging are fixed to the conductive tracks of the circuit by a conductive glue which is, for example, isotropic.

[00133] The type of printed circuit used in accordance with the invention that can be permanently fixed to a printer cartridge is of the type sold by the company Parlex, for example.

[00134] Figure 4a shows diagrammatically a standard inkjet printer cartridge 46, for example a Hewlett Packard HPc665x cartridge.

[00135] As the person skilled in the art knows, the cartridge contains an ink

reservoir and a print head 50 with nozzles for ejecting ink onto the support to be printed.

[00136] As the person skilled in the art also knows, the cartridge has on its exterior surface electrical contacts 79 mounted on a thin circuit affixed to the cartridge, the electrical contacts being adapted to route the printing control signals to the print head to control the ink ejector nozzles.

[00137] Note that standard cartridges available off the shelf have no onboard intelligence and that in this case the printing control signals are therefore transmitted to the print head without analysis, in contradistinction to the present invention.

[00138] As shown in Figures 4b, 4c and 4d, the inkjet printer cartridge 46 shown in Figure 4a is fitted with the identification tag previously described (the identification module 58 shown in Figures 1 and 2), for example by permanently gluing it to the exterior surface of the cartridge.

[00139] It is important for the substrate 60 of the identification tag to be fixed permanently to the cartridge, so that any subsequent attempt to remove the substrate, damages the communication means 62, 64 on it.

[00140] If the communication function of the identification tag is damaged, this makes it impossible for the source of confidential and/or sensitive data, for example the unit 12 for generating franking data in Figure 1, to identify the printer cartridge concerned.

[00141] The person skilled in the art knows how to fix the substrate permanently to the cartridge, for example using glues available off the shelf, suited to the materials to be in contact, and providing a particularly intimate contact between the substrate and the exterior surface of the cartridge (Figures 4c and 4d).

[00142] As can be seen in the Figures, the identification tag 58 can be larger than a face 85 of the cartridge. In this case, thanks to the flexibility of the tag, it can be folded and one portion of the tag positioned on the face 85 and the other portion folded onto one of the adjacent faces 86 of the cartridge.

[00143] Once again, the identification tag 58 is particularly thin, enabling it to be integrated onto the exterior surface of the cartridge without modifying the overall external size of the latter to a degree that would compromise the installation of the cartridge in a standard printer unit.

[00144] The constraints on the thickness of the identification tag are the same as those previously indicated for the intelligent module 54.

[00145] The thickness of the tag is less than 1 mm, for example.

[00146] As shown in Figures 4e to 4h, the Figure 3 printed circuit 66 is permanently fixed to the exterior surface of the printer cartridge to prevent insertion of an external element between the circuit and the cartridge itself.

[00147] To this end, the circuit 66 can be glued intimately to the exterior surface of the cartridge, for example, so that any attempt to remove the circuit 66 by unsticking it damages it and therefore makes it impossible for a fraudster to use the cartridge.

[00148] More particularly, the second portion 69 of the thin printed circuit 66 carrying the data processing unit 68 is first applied to one of the exterior faces 81 of the cartridge (see Figure 4f), while the first portion 67, carrying the electrical contact areas, is applied to an adjacent face 83 of the cartridge (see Figures 4g and 4h).

[00149] It will be noted that the second portion 69 of the thin circuit 66 is preferably affixed to a region of the exterior surface of the cartridge which, when the cartridge is integrated into a printer unit, defines with the components of the printer unit sufficient space to accommodate the data processing unit 68.

[00150] Accordingly, assuming that, when the printer cartridge is integrated into a printer unit, the space in front of the external faces of the cartridge is larger in front of the face 85 of the cartridge that is opposite the face 83, it is then possible for the circuit 66 to extend from the face 83 as far as the opposite face 85 and for the data processing unit 68 to be positioned facing that face.

[00151] Of course, in this situation, the identification tag 58 must then be positioned on another free region of the exterior surface of the printer cartridge.

[00152] It should be noted that the flexibility of the modules 54 and 58 is optimally exploited so that these modules can espouse the available exterior surface of the cartridge as closely as possible.

[00153] Thus the flexibility of each module enables it to adapt to the geometry of the cartridges and to the constraints associated with the installation of the cartridges into their support in the printer unit.

[00154] However, in some applications, flexibility of one or both of the two modules

54 and 58 is not a requirement, and consequently it suffices for the module or modules to be thin.

[00155] Note that, when the intelligent module 54 (or the identification module 58) is affixed to a single face of the cartridge according to the invention, the property of flexibility of the corresponding module is less important, and may even not be necessary.

[00156] Thus the disposition of the thicker portion of the Figure 3 intelligent module 54 depends on the free space around the printer cartridge when it is installed in a printer unit.

[00157] Note that the Figure 4h inkjet printer cartridge 46 is equipped with an identification module enabling an external device (a source of confidential and/or sensitive data) to identify the cartridge, and with an intelligent module, these modules each having particular means of making the cartridge secure.

[00158] Note that the inkjet printer cartridge according to the invention can be used in other applications in which it is not necessarily equipped with the identification module 58.

[00159] Equipment of the above kind affixed to a standard inkjet printer cartridge available off the shelf is particularly advantageous in that it does not call into question the design of the cartridge or its overall outside dimensions.

[00160] The inkjet printer cartridge according to the invention, equipped with an intelligent module 54, and where applicable with an identification module 58, can be used outside the field of franking machines, and in particular in printer units that receive confidential and/or sensitive data from exterior devices.

[00161] In the Figure 1 franking machine, the data is made secure firstly by the authentication of the printer cartridge 46 by the data generating unit 12.

[00162] To this end, the unit 12 obtains data identifying the print member 46 using the wireless communication mode described above.

[00163] When the central unit 18 of the unit 12 has verified that the print member 46 is an authorized printer cartridge, the module 20 then generates a franking data signature using a mathematical method known to the person skilled in the art. The encryption circuit 22 of the module 20 then encrypts the signature generated in this

way, for example using 3DES encryption, which is known to the person skilled in the art.

[00164] This kind of encryption requires the sender and the receiver to hold different encryption keys that are 128 bits long in the case of 3DES encryption.

[00165] Because decryption is effected in the processing unit 68 of the module 54, a key is written into the unit 68 when manufacturing the module 54.

[00166] This key must also be known to the sender, and therefore contained in the encryption circuit 22.

[00167] The sender 12 uses the key to encrypt the data and the receiver 54 uses it to decrypt the data.

[00168] The key can be programmed when installing the module 54 on the printer cartridge or programmed directly into the processing unit 68 during manufacturing of the module 54.

[00169] When the signature is encrypted, the unit 18 associates with it, for example concatenates with it, franking data and transmits the whole of the data, which constitutes the stream 42, over the communication link 38.

[00170] Note also that, in the embodiment described, there is no encryption as such of the franking data to be printed, although this is of course possible in a different embodiment.

[00171] Franking data to be printed can additionally be encrypted, which makes the exchange of this data between the unit 12 and the printer unit 14 more secure.

[00172] However, encryption should not be used if it necessitates too great a volume of computation, in that the processing unit 68 of the module 54 diverts the energy necessary for it to function from the printing control signals reaching it.

[00173] Figure 5 shows diagrammatically functional units of the Figure 3a data processing unit 68.

[00174] As shown in Figure 5, the data processing unit 68 receives the Figure 1 stream of printing commands 44 and analyzes it, in particular to authenticate the data to be printed.

[00175] As mentioned above, the energy necessary for the processing unit to function is diverted from the stream of printing control signals.

[00176] The data processing unit could use a microprocessor provided that there is

no risk of the energy diverted degrading the printing of data.

[00177] Thus the processing unit 68 includes a self-powering unit 92 and a clock generator unit 94 that supply a particular clock frequency to each of the various units described next.

[00178] A unit 96 extracts the encrypted signature from the stream 44 of printing commands reaching the data processing unit 68 and decrypts this signature.

[00179] This is possible because the encryption key or keys are also known to the processing unit 68, because they are programmed either during manufacturing of the module 54 or when it is affixed to the print member 46.

[00180] Decryption is effected by the decryption unit 98.

[00181] The data processing unit 68 also includes a circuit 99 that includes an authentication unit 100 for authenticating the data to be printed on the basis of the analysis of the decrypted signature of the franking data.

[00182] As a matter of fact, when the unit 100 registers the presence of the signature of the franking data in the stream of printing commands, this proves the authenticity of the data to be printed.

[00183] Note further that the unit 12 for generating franking data is thereby indirectly authenticated by the printer cartridge.

[00184] It is possible to use only one level of verification, and thus to decide to authorize the printing of data as soon as the data to be printed has been authenticated.

[00185] A supplementary level of verification can also be provided, by way of the unit 102 that verifies the integrity of the data to be printed to check that, even if the data comes from an authentic source, it has not been tampered with after leaving the source.

[00186] To this end, tests are applied to the data present in the stream of printing commands.

[00187] When the integrity of the data to be printed has been recognized, then the unit 104 authorizes printing of the data.

[00188] On the other hand, if the data has not been authenticated by the unit 100 or the integrity of the authenticated data has not been recognized by the unit 102, then the unit 104 decides either not to authorize printing of the data or to generate an erroneous

and therefore unusable franking mark.

[00189] To be more specific, note that the data processing unit 68 first prints a few lines of franking data, for example, and then analyzes some of the data extracted from the stream of printing commands, after which, as a function of the result of the analysis, it can authorize the printing of further lines and again analyze other data extracted from the stream of printing commands, and so on.

[00190] It should be noted that the data processing unit 68 also includes a non-volatile memory 106 whose main function is to store the dynamic values of the application, for example the cartridge manufacturing date, and the like, and where applicable to store values generated by the units 98, 100 and 102.

[00191] Figure 6 shows in more detail some of the components constituting the Figure 5 data processing unit 68.

[00192] The data processing unit 68 includes a serial receiver unit 108 notably including a buffer memory for the intermediate storage of data extracted from the stream 44 of printing control signals.

[00193] As shown, some of the printing control signals are used by unit 92 for self-powering the data processing unit 68.

[00194] A unit 110 for analyzing data extracted from the printing control signals and combining various functions executed by the units 98, 100, 102 and 104 in Figure 5 supplies a signal Cmd-decode.

[00195] A circuit 112 including a logic switch selectively authorizes the passage of a signal Xout, on the basis of a printing control signal Xin, as a function of the value of the control signal Cmd-decode.

[00196] The Cmd-decode signal is produced for one or more lines of franking data and, for example, authorizes the passing and therefore the printing of a given number of lines of franking data that constitute the franking mark.

[00197] Note that the circuit 112 constitutes a pattern that is repeated several times according to the number of signals Xin obtained from the printing control signals.

[00198] The stream 114 of printing commands from the unit 68 is then transmitted to the print head 50 to control the print nozzles.

[00199] Figure 7 shows diagrammatically the self-powering principle of the Figure 6

unit 92.

[00200] Thus the Figure 7 circuit 120 includes a set 122 of (m) diodes in parallel and each receiving one of the control signals Cmd cartridge 0 to Cmd cartridge m, each of which corresponds to data specific to one line of the image to be printed.

[00201] The set 122 of diodes implements an "OR" logic function which therefore authorizes the delivery of a signal when its state is 1.

[00202] The control signal that is allowed to pass is then filtered in a filter 124 in which the values of the components R, C are determined as a function of the value of the "load" of the circuit of the unit 68, to allow the accumulation of energy.

[00203] Figure 8 shows timing diagrams for loading the unit 68.

[00204] Thus, as shown by the evolution of the output signal Vout of the self-powering unit, the latter signal is generated (portion a) by the detection of a first rising edge of a control signal Cmd cartridge x. When that control signal goes to 0, the self-powering signal Vout loses a little energy (portion b), but the energy level begins to rise again (portion c) after the detection of a rising edge of the next control signal Cmd cartridge x+k.

[00205] Note also that the control signals generated by the unit 12 and intended for controlling the print head 50 can have an amplitude of the order of 20 V, and the processing unit 68 therefore uses a high-voltage technology.

[00206] The core of the unit 68, which is an application-specific integrated circuit (ASIC), for example, operates at a voltage of 3.3 V or 5 V, for example, and incorporates memory in the form of RAM or EEPROM.